We claim:

1. A method of authenticating the identity of a user, the method comprising:

a. placing, in sequence, each of a plurality of parts of the user's body on a biometric contact sensor at a sensing position;

b. obtaining from the sensor a data set of biometric contact characteristics for each of the plurality of body parts;

c. comparing each data set with authentic versions stored in a database; and,

d. issuing an authentication signal if the data sets satisfactorily match the corresponding authentic versions.

2. A method according to claim 1, wherein the body parts are the user's fingertips and the biometric contact sensor is a fingerprint sensor.

3. A method according to claim 1, wherein each part of the user's body must be placed on the biometric contact sensor within a predetermined time period before the authentication signal will be issued.

4. A method according to claim 1, further comprising the step of confirming that the sequence of data sets was obtained in a predetermined order before issuing the authentication signal.

5. A method according to claim 1, wherein the data sets are compared with the authentic versions using a minutiae based algorithm.

6. A method according to claim 1, wherein the data sets are compared with the authentic versions using a correlation based algorithm.

7. Apparatus for authenticating a user, the apparatus comprising a fingerprint sensor capable of sensing only one fingerprint at a time, and a processor and a database adapted to perform a method according to claim 1.

8. Apparatus according to claim 7, wherein the fingerprint sensor is a capacitive sensor.

9. Apparatus according to claim 7, wherein the fingerprint sensor is an optical sensor.

10. Apparatus according to claim 7, wherein the fingerprint sensor is a thermal sensor.

11. Apparatus according to any of claim 7, further comprising a data input device.

12. Apparatus according to claim 11, wherein the data input device is a keypad.

13. Apparatus according to claim 11, wherein the data input device is a smart card reader.

14. A method of authenticating the identity of a user, the method comprising:

a. obtaining a sequence of data sets of biometric characteristics of the user, each data set relating to one of a plurality of parts of the user's body;

b. comparing each data set with authentic versions stored in a database;

c. monitoring the order in which the sequence of data sets was obtained; and,

d. issuing an authentication signal if the data sets satisfactorily match the corresponding authentic versions and the sequence of data sets was obtained in a predetermined order.

15. A method according to claim 14, wherein at least one of the plurality of parts of the user's body is a fingertip.

16. A method according to claim 14, wherein at least one of the plurality of parts of the user's body is a retina.

17. A method according to any of claim 14, wherein at least one of the plurality of parts of the user's body is the user's face.